SCHEDULE L: SERVICE DEFINITION FOR MICROSOFT SENTINEL CYBER SECURITY OPERATIONS CENTRE SERVICES

1. Service Description for Microsoft Sentinel Cyber Security Operations Centre Services

Vysiion Microsoft Sentinel Cyber Security Operations Centre Services (Microsoft Sentinel CSOC Service/s) comprises all of the Service packages detailed in section 3 below and will be provided by Vysiion from its Cyber Security Operations Centre (CSOC).

The Security Information and Event Management (SIEM) used for this Service is Microsoft Sentinel.

The Order Form will set out the number of committed security incidents per instance covered by the Charges for that instance on the Order Form. Any incidents beyond the committed number of security incidents set out in the Order Form will be at additional charge to the Customer and be invoiced monthly in arrears in accordance with the then current Rate Card (available upon request from sales@vysiion.co.uk).

A Statement of Work (SoW) will support each engagement. The SoW contains the timescales for deliverables (such as reports or system outputs and analysis), and any target service level for monitoring the Services. Once signed by both Parties, the SoW is deemed to form part of the Contract. The definition of Contract in the General Terms shall therefore be considered amended accordingly. In the provision of all Microsoft Sentinel CSOC Services, Vysiion acts as a consultant providing advice to the Customer in relation to the security of its estate. Vysiion will not be liable for any failure to meet any target service levels where such failure arises as a direct or indirect result of changes which the Customer may implement. Changes made by the Customer are made at the Customer's sole risk. It is the Customer's responsibility to qualify the impact of any potential change and to satisfy itself that the change is required, actionable and supportable for the security of its estate.

Microsoft Sentinel licensing is not part of this Service. The Customer must bring the Microsoft Sentinel Licensing. This can be purchased through Vysiion or another Microsoft Cloud Service Provider.

2. On boarding and Engagement

Vysiion will collect all the relevant information to create the SoW for each Microsoft Sentinel instance (an instance is the deployment by Vysiion of the Customer's Microsoft Sentinel licensing connected to an Azure Log Analytics workspace, each instance would require a separate workspace). Once the Customer has accepted the SoW, the provision of Microsoft Sentinel CSOC Service will begin and it will be considered complete when the Microsoft Sentinel instance receives its first log. The number of Microsoft Sentinel instances and associated components deployed in respect of the Customer will depend on the number of assets to be monitored and the quantity of zones (i.e. whether the Customer's servers are located in more than one location namely; Azure, AWS and at data centres). The number of Microsoft Sentinel instances to be deployed will be set out on the Order Form..

As per above, the Service Commencement Date is deemed to have occurred in relation to the Microsoft Sentinel CSOC Service once the first log is ingested/collected by the Microsoft Sentinel instance. Where servers are included in the scope (as detailed within the SoW), a Windows Agent will need to be deployed on any Microsoft server, in order to enable SIEM logging and monitoring, by the Customer unless Vysiion is managing that Microsoft server as part of a Flex Manage Service. Devices such as firewalls that generate syslog, as well as other solutions that might provide an API integration, may require additional servers to facilitate log collection. Vysiion will also set out in the SoW the agreed list of activities for each Party for the alerts that are detected. The Customer will be provided with credentials to have a read-only view of the Microsoft Sentinel instance on the Azure portal. In the event that following on boarding there is an alert, CSOC will respond to the Customer as agreed in the SoW, subject always to the severity of the incident monitored. The Parties will also discuss on a weekly basis during the on-boarding stage, at a time agreed between the Parties, the output logs and the variations which occur in the logs. CSOC will refine and tune these output logs throughout the on boarding stage. During the course of the engagement and at a time agreed with the Customer and no more than on a quarterly basis, a CSOC engineer will have a telephone discussion with the technical contact of the Customer to discuss the technical operation of the Service. If during the engagement, a monitored asset which forms part of another service which Vysiion is providing to the Customer has a fault, CSOC will notify the Customer and the relevant Vysiion support team who will then liaise with the Customer as set out in the applicable Service Document for the affected Vysiion service.

3. The Cyber Security Operations Centre Services Packages

a) Security Incident and Event Monitoring (SIEM)

The SIEM consists of at least one Microsoft Sentinel instance. This instance will collect log information from the Customer's monitored assets. This provides a view via the Azure portal of the Customer's assets within scope of the SoW. The Microsoft Sentinel instance is deployed in the Customer's Microsoft Azure public cloud environment. Azure resources are not part of this Service. The Customer must bring the required Azure resources. This can be purchased through Vysiion or another Microsoft Cloud Service Provider.

The Customer acknowledges and accepts that any failure on its part to allow for the installation of Microsoft Sentinel instance and the required alerting and monitoring components for the integration with Vysiion systems will result in none of its assets being monitored by Vysiion.

b) Threat Detection

Vysiion will alert and monitor the Customer's estate for triggered threats. This is a service consisting of a deployed Microsoft Sentinel instance and the proactive monitoring of the Customer's estate, as defined in the SoW, on a 24x7x365 basis. The result of the monitoring consists of ServiceNow cases, available on the dashboard, flagged with the respective severity level (S1-S4). CSOC will provide the Customer with further intelligence via ServiceNow case about the incident in order to support remediation.

4. Monitoring

The Microsoft Sentinel CSOC Service adopts the analytics rules that are part of the baseline, as defined on the SoW, and any additional that may be included in scope. Regular reviews of the rules should take place to ensure that they continue to offer the best protection for the environment.

5. Change Management

Changes requested will be limited to a change of priority notification or change of monitored devices and will only be carried out during Normal Business Hours. In the case that a new device type is introduced to the Microsoft Sentinel CSOC Service, the CSOC won't be required to ensure that any agreed SLA of alerts, stated in the SoW, are met until a pre-agreed tuning period is completed, during this time the Customer will regress to a Staging period instead of a Live status. Staging period being the period during which Vysiion will monitor the SIEM to understand what changes, if any, is required to the Microsoft Sentinel CSOC Service before handover.

6. Access and Reporting

The Azure portal enables read-only access to the Microsoft Sentinel instance so that the Customer can obtain further information on a particular incident.

7. Target Service Commencement Date

The Target Service Commencement Date will be set out in the SoW and shall be calculated from order acceptance. The Customer accepts that where Vysiion agrees to delay the Service Commencement Date following the Customer's written request, or the Target Service Commencement Date is not met as a result of the Customer's delay or failure to fulfil its obligations in respect of this Service or under the Contract, the Annual Charges for that Service shall be payable by the Customer from the Target Service Commencement Date set out in the SoW, unless otherwise agreed in writing between the Parties. For the avoidance of doubt, notwithstanding any agreement by Vysiion to delay the Service Commencement Date following the Customer's written request, the Service Commencement Date will be deemed to have occurred on the earlier of: (a) fourteen (14) days after the first log is ingested/collected by the Microsoft Sentinel instance and (b) thirty (30) days from Order Form acceptance. Accordingly, the Annual Charge shall be deemed payable from that Service Commencement Date. Nothing in this clause shall oblige Vysiion to agree to any delayed handover of this Service.

8. Incident Logging

For incidents logged to the CSOC by the Customer, the priority can be set by the Customer acting reasonably in line with the below definitions, when logging the incident with Vysiion.

Severity Level	Description
S1	A critical business service is non-operational impacting the Customer organisation, multiple users or multiple sites; or severe functional error or degradation of service affecting production, demanding immediate attention. Business risk is high, with immediate financial, legal or reputational impact.
S2	The Customer is experiencing failure or performance degradation that severely impairs operation of a critical business service; or the Customer or service has been affected, although a workaround may exist; or application functionality is lost; or significant number of users or major site is affected. Business risk is high.
S3	The Customer is experiencing a problem that causes moderate business impact. The impact is limited to a user or a small site; or incident has moderate, not widespread impact; or the Customer or IT service may not have been affected. Business risk is low.
S4	Standard service request (e.g. User Guidance); or updating documentation. Low or Minor localised impact.

9. Additional Terms applicable to the Microsoft Sentinel CSOC Service

9.1. In addition to the reasons set out in section 6.2 of the main body of this document, Vysiion shall also have no liability for any failure to meet the Target Service Commencement Date and/or target service levels due to, or as a result of, any of the following reasons:

- Change management requirements affecting monitored devices
- Network or policy changes to a monitored device not performed by Vysiion
- Loss of connectivity due to Customer connectivity issues or Customer managed issues
- Requirements which the Customer must meet before the Service can be provided and during its provision as set out below ("Customer Dependencies").

9.2. Customer Dependencies

9.2.1. The Customer shall ensure that:

a) Each device covered by the Service has the appropriate full manufacturer's product licence and subscriptions for the duration of the Service. Software and devices that are considered end of life by the manufacturer are not covered by the Service; and

b) All devices must have full manufacturer's support for the duration of the Service.

9.2.2. The Customer accepts the following as a condition of Vysiion providing the Service:

a) The Customer is expected to adopt best practice cyber security regime within its business;

b) Vysiion is not responsible for resolving the Customer's Internet Service Provider (ISP) outages, or issues with the Customer's internal network or computing platform infrastructure where Vysiion is not contracted to support those elements; and

c) It is the responsibility of the Customer to ensure the log stream is directed at Microsoft Sentinel instance for Service operation where applicable.